

**RESPONSE UNDER 37 C.F.R. 1.116
EXPEDITED PROCEDURE EXAMINING GROUP 2135**

Attorney Docket No. RSW920010222US1 (5577-351)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Brabson et al.
Serial No.: 10/007,582
Filed: December 5, 2001
For: OFFLOAD PROCESSING FOR SECURE DATA TRANSFER

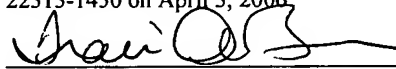
Confirmation No.: 3561
Examiner: Joseph T. Pan
Group Art Unit: 2135

Date: April 3, 2006

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Mailing under 37 CFR § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 3, 2006.


Traci A. Brown

**REASONS IN SUPPORT OF APPLICANTS' PRE-APPEAL
BRIEF REQUEST FOR REVIEW**

Sir:

This document is submitted in support of the Pre-Appeal Brief Request for Review filed concurrently with a Notice of Appeal in compliance with 37 C.F.R. 41.31 and with the rules set out in the OG of July 12, 2005 for the New Appeal Brief Conference Pilot Program.

No fee or extension of time is believed due for this request. However, if any fee or extension of time for this request is required, Applicants request that this be considered a petition therefor. The Commissioner is hereby authorized to charge any additional fee, which may be required, or credit any refund, to IBM's Deposit Account No. 09-0461.

REMARKS

Applicants hereby request a Pre-Appeal Brief Review (hereinafter "Request") of the claims finally rejected in the Final Office Action mailed January 3, 2006 (hereinafter "Final Action"). The Request is provided herewith in accordance with the rules set out in the OG dated July 12, 2005.

Applicants respectfully submit that many of the recitations of the pending claims are not met by the cited reference for at least the reasons discussed herein and in Applicants' previously filed Amendment of October 19, 2005. Therefore, Applicants respectfully request review of the present application by an appeal conference prior to the filing of an appeal brief. In the interest of brevity and without waiving the right to argue additional grounds should this Petition be denied, Applicants will only discuss the recitations of independent Claims 1, 12, and 13, and dependent Claims 8 - 11 and 17. Applicants further submit that the rejection of all pending claims under 35 U.S.C. § 112, first paragraph is erroneous for at least the reasons discussed below.

The 35 U.S.C. § 112 Rejection

Claims 1 - 20 stand rejected under 35 U.S.C. § 112, first paragraph. In particular, the Final Action alleges that the recitations of independent Claims 1, 12, and 13 clarifying that the security offload component is "in an operating system kernel" are new matter. Applicants respectfully disagree. As explained in Applicants response dated October 19, 2005, the first sentence in the "DESCRIPTION OF PREFERRED EMBODIMENTS" states: "[t]he present invention moves security processing (or control thereof) for security protocols such as SSL and TLW (which are connection-oriented protocols) into the kernel." (Specification, page 11, lines 13 - 14). The Specification further explains that the use of a "security offload component" is exemplary of some embodiments in which the security processing is moved to the operating system kernel. (Specification, page 11, lines 15 - 17). Thus, Applicants submit that the recitations of independent Claims 1, 12, and 13 clarifying that the security offload component is "in an operating system kernel" are not new matter and that Claims 1 - 20 satisfy the requirements of 35 U.S.C. § 112.

The 35 U.S.C. § 102 Rejection

Independent Claims 1, 12, and 13 stand rejected under 35 U.S.C. §102(e) as being anticipated by U. S. Patent No. 6,175,917 to Arrow et al. (hereinafter "Arrow"). (Final Action, page 4). Independent Claims 1, 12, and 13 are directed to a method, a system, and a computer program product for improving security processing in a computing network in which a security offload component is used. These three claims include recitations that state that the security offload component is in the operating system kernel. For example, independent Claim 1 recites:

providing a security offload component in an operating system kernel
which performs security processing;
providing control functions in the operating system kernel for directing
operation of the security offload component;
providing an application program;
executing the application program; and
executing the provided control functions during execution of the
application program, thereby selectably directing the security offload component
to secure at least one communication of the executing application program.
(Emphasis added.)

Claims 12 and 13 include similar recitations. Support for providing the security offload component as part of the operating system kernel is provided, for example, at page 11, lines 13 - 19 of the Specification. The Final Action cites the encryption/decryption unit 730 shown as a component of the operating system 116 in FIG. 7 of Arrow as disclosing the security offload component recited in independent Claim 1. (Final Action, page 4). Applicants acknowledge that Arrow describes an operating system 116 with respect to FIG. 7 in which security processing is shown as being performed by the encryption/decryption unit 730. **In sharp contrast to the recitations of independent Claims 1, 12, and 13, however, the encryption/decryption unit 730 of Arrow is not part of the operating system 116 kernel, which appears to be the VPN processor 718 as it is described as controlling "the operation of the operating system 116."** (Arrow, col. 10, lines 56 - 58). Moreover, Arrow explains that, in some embodiments, the encryption/decryption unit 730 is implemented as an application specific integrated circuit (ASIC). (Arrow, col. 11, lines 43 - 47). Applicants, therefore, respectfully submit that Arrow appears to contain no disclosure or suggestion of incorporating the encryption/decryption unit

730 in the VPN processor 718, which appears to serve as the operating system 116 kernel.

Applicants submit, therefore, that Arrow does not disclose, at least, the recitation **"providing a security offload component in an operating system kernel** which performs security processing" of Claim 1. Moreover, Claims 12 and 13 include similar recitations. Therefore, Applicants respectfully requests that the present application be reviewed and the rejection of independent Claims 1, 12, and 13 be reversed by the appeal conference prior to the filing of an appeal brief.

Various Dependent Claims are Separately Patentable

Dependent Claims 8 - 11 are patentable as least as they depend from patentable independent Claim 1 and dependent Claim 17 is patentable at least as it depends from patentable independent Claim 12. Applicants further submit, however, that these dependent claims are separately patentable for at least the reasons discussed hereafter.

Dependent Claims 8 - 11 stand rejected under 35 U.S.C. §102(e) as being anticipated by Arrow. Each of dependent Claims 8 - 10 provides additional details with respect to what is provided to the security offload component for use in securing communications. Dependent Claims 11 and 17 provide additional detail with respect to how outbound data is sent from the security offload component. Arrow's description of the encryption-decryption unit 730 appears to be limited to the passage at col. 11, lines 43 - 47, which does not include any details with respect to what the encryption-decryption unit 730 uses to provide secure communications or how data is sent from the encryption-decryption unit 730.

In response to this argument, the Final Action cites the passage of Arrow at col. 2, lines 34 - 43, which states, in part:

The operating system of an encryption of decryption device, for example, may include instructions detailing the method of encryption or decryption to be applied, identifying how to differentiate between streams of data that are and are not to be encrypted or decrypted.

Applicants submit that the foregoing passage from Arrow does not contain any description of the detailed security techniques recited in dependent Claims 8 - 11 and 17. The passage from Arrow reproduced above merely states that the operating system may identify the method of

encryption/decryption used and how to differentiate between data that is to be encrypted/decrypted and data that does not need such processing. No mention is made with regard to specific techniques, such as, for example, client and/or server certificates, one or more keys/key rings, algorithm identification, and/or sending outbound data directly to a destination from a security offload component as recited in dependent Claims 8 - 11 and 17.

Accordingly, for at least the additional reasons discussed above, Arrow does not disclose the recitations of dependent Claims 8 - 11 and 17. Therefore, Applicants respectfully request that the present application be reviewed and the rejection of dependent Claims 8 - 11 and 17 be reversed by the appeal conference prior to the filing of an appeal brief.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Scott Moore", written over the printed name.

D. Scott Moore

Registration No. 42,011

USPTO Customer No. 46589

Myers Bigel Sibley & Sajovec

Post Office Box 37428

Raleigh, North Carolina 27627

Telephone: (919) 854-1400

Facsimile: (919) 854-1401